名古屋女子大学　紀要　**51**（人・社）29～34　2005

統合ユーザー認証システムの構築

学術情報センター

Construction of an integrated user authentication system

Library and Science Information Center

はじめに

本学ではコンピュータ演習室に平成 9 年から LAN を構築している。個人情報保護、セキュリティという言葉が叫ばれている中、ようやく平成16年 4 月にコンピュータ演習室における個人認証を導入した。それまで学生はコンピュータ演習室を利用するとき、共通ユーザー、共通パスワードを利用しており、結果的としてセキュリティなどないに等しい状況であった。個人認証システム導入の必要性と実現方法について述べる。

目的

2003年 3 月まで本学のコンピュータ演習室では、共通ユーザー、共通パスワードを利用していた。これは文字通りすべてのユーザーが同じユーザー名、パスワードを利用するということである。ただしメールという個人の情報にアクセスするときは、個々のパスワードを利用していた。

しかし､これではどのユーザーが､パソコンを利用したかは把握できない。また個人用のホームディレクトリを提供することができないので、データ保存用の FD か MO を持ち歩く運用方法であった。

この状況でも、通常運用時は特に問題はなかったが、ひとたび問題 --- 不正アクセスなど --- が起きると追跡の方法がなかった。また、FD や MO を常に持ち歩くため破損があり、データが読めないということもしばしばあった。

そこで個人認証を導入することによって、ユーザーの利用履歴管理ならびにホームディレクトリを提供することとした。これによりどのユーザーがどのパソコンを利用したかを追跡できるようになり、また必要時以外は FD や MO などのメディアを持たなくてよい状況とする。

個人認証導入にともなう問題点

個人認証導入にあたって、当時のシステムでは以下のような問題点があった。

コンピュータ演習室での個人認証に使うパスワードと、メールを受信するときのパスワードの 2 種類を覚えなくてはならない。このとき演習室のユーザー管理は Microsoft の Windows NT Server 4.0でNTドメインを組んで行っていた。一方メールは、Sun Microsystem の Solaris 上にメールサーバを構築し、POP を使って受信していた。

このパスワードを連携させるかどうが、システムの構築の鍵を握っていた。

技術者の対場からすると 2 つのまったく異なるシステムのパスワードを 2 つ使い分けるのは簡単である。しかし、すべての学生が、コンピュータ演習室利用時とメール受信時という 2 つの違いを理解して使用するとは思えない。

これを解決するには、コンピュータ演習室利用時のパスワードとメール受信時のパスワードの同期が必要になる。この当時、Windows と Solaris をはじめとする UNIX とのパスワード同期はいくつかの方法があったが、それらを導入できるだけの知識は担当者にはなかった。

パスワードの同期を行わず、個人認証だけを導入するのはそれほど難しくない。同期を行うとなると一気にハードルが高くなるのである。

システムに求める担当者の要求は以下のとおりである。

・コンピュータ演習室利用時とメール受信時のパスワードを一つとする。
・なるべくシンプルなシステムなものとする。

この 2 点から考えるとその当時、すでに製品化されていた Windows 2000 Server を用いての Active Directory の構築だった。この方法ならコンピュータ演習室管理をいままでどおり Windows で行い、メールサーバである UNIX 系 OS との連携も可能である。

検討している中 Windows Server 2003が登場し、コンピュータ演習室は Windows Server 2003 を用いた Active Directory を構築することにした。

導入の方法

Windows NT Server から Windows 2003 Server への移行には、以下の方法がある。

・既存の NT ドメインをアップグレードする。
・新規に Active Directory ドメインを構築する。

このうち、担当者としては後者を選択した。

既存の NT ドメインをアップグレードする方法でもよいが、NT ドメインから新しい Active Directory ドメインへ移行する情報が少ないことと、新規に作成したほうが構築が簡単なことから後者を選択した。

新規 Active Directory ドメインは以下のような構成とした。

・ドメインコントローラ× 3 台
・DNS サーバ× 3
・ファイルサーバ× 3

このうちドメインコントローラと DNS サーバは 1 台で双方のサーバを兼ねている。

さらにドメインコントローラの内の 1 台は、FSMO（Flexible Single Master Operation）と呼ばれ核となるサーバとなる。このサーバに対して UNIX システムのメールサーバはクライアントからの要求に従ってパスワードの認証を行う。またこのサーバは、新図書館システムからも利用されることになっている。

ファイルサーバには学生、教員のホームディレクトリが置かれ、コンピュータ演習室から利用することができる。学生はこのディレクトリに、自分のデータやメールデータを置いて利用している。また教員からは教材の提供や課題の提出に利用している。

結果

この個人認証システムを導入することによって以下のことが可能となった。

・個人認証によるユーザーの利用状況の管理。
・ホームディレクトリ提供による利便性の向上。

1 点目は、本来の目的であるユーザーの履歴管理である。ログを見ることによってどのユーザーがどのパソコンを利用したかを必要があれば追跡することが可能になった。

2 点目は、ホームディレクトリを提供することによって、従来使用していた FD や MO を利用しなくてもよくなったことである。コンピュータ演習室でコンピュータにログインをすれば自分のデータを使用することが出来るようになった。

このように個人認証を導入することによって、セキュリティ面、利便性を大きく向上させることが可能になった。

メールサーバの構築

組織的にメールサービスを提供する場合、一般ユーザーが利用する端末は Windows を使用する場合が多く、またメールサーバのような基幹システムは UNIX（及び UNIX 互換 OS）が採用される場合が多い。これら異なるシステム間のパスワードの統一化は従来から難易度の高い問題として扱われ、同じアカウント名でもまったく別のユーザとして管理する運用が行われてきた。SFU（Service for UNIX）[1]を用いて UNIX 側とパスワードの同期を行う方法はあったが、一元的に管理を行っているわけではないことと、対応 OS が限られることから採用は難しかった。しかし LDAP（Lightweight Directory Access Protocol [2] をベースとした Active Directory [3]の登場により、認証の一元化についての選択肢が広がった。ここでは我々が行ったメールサーバ構築方法についての概要を説明する。

何故 Active Directory なのか

統合認証を考えたとき、どのプラットフォームにて認証を行うかで全体の構成が変わってしまう。Active Directory 以外に NDS [4] や OpenLDAP [5]、OpenDirectory [6] といったディレクトリサーバは存在し、samba 等を用いることによって Windows 端末への認証を含めた統合認証環境は技術的には可能である。しかし、logon スクリプトやプリンタ、ポリシー制限などこれまで蓄積した Windows における管理方法が実現不可能になる可能性もある。Active Directory はそれ自体にライセンス料は必要なく、導入事例も他のディレクトリサーバと比較して多いため、導入にあたっての懸念材料は少ない。

Active Directory との連携について

Active Directory は LDAP をベースにしたものであるが、外部からの認証を行う場合、Kerberos [7] を用いることが推奨されている [8]。そのため、各ユーザーからメールの受信要求があった場合、POP 3 サーバ [9] が Kerberos を用いて Active Directory に対して個人認証を行う必要がある。しかし Kerberos をサポートしている POP 3 サーバが限られるため、OS 側にて Kerberos 認証を行う方法を検討した。

PAM

PAM（Pluggable Authentication Module）とは、従来アプリケーション毎で実装が必要であったユーザー認証をモジュール化することにより、さまざまな認証技術を OS 側で一元的に統合管理するものである。認証を必要とするサービスはそれぞれ PAM 設定ファイルを通して、異なる認証方式を使うように設定できる。POP3サーバは PAM をサポートしていれば認証方法は様々な方法を選択することが可能になる。今回は PAM が Kerberos 認証をサポートすることによって、ActiveDirectory を POP3サーバの認証に利用できる。（図1）

サーバの多重化

今回メールサーバの更新は教員用及び学生用のメールサーバが対象となる。これまでは別のハードウェアにて運用を行っていたが、近年 PC の性能が飛躍的に向上しており、Hyper-Threading[10]や RAID 1[11]により高性能化・高信頼性を図ることができるため、1 台に集約しても性能的には問題がないと判断した。

実現

上記の条件を満たす OS として PC-UNIX の雄である FreeBSD を選択した。FreeBSD はエンタープライズ向けとして各方面にて利用されており信頼性が高い。FreeBSD は HEIMDAL Kerberos を標準で実装しており、Active Directory との認証統合については実績があった。また jail[12]と呼ばれる機構を用いることによって、一台のホスト OS 上に複数のゲスト OS を稼動させることが可能になる。ゲスト OS 間はプロセスも分離されているため、仮に諸問題が起きても他のゲスト OS への影響は少ない。またゲスト OS 上の管理者権限は制限されているため安全性も高い。

統合ユーザー認証システムの構築として、Active Directory を認証サーバとしたメールサーバの構築について述べてきた。今回にてパスワードを一元的に管理することにより利用者の安全性と利便性の向上を図ることができた。しかし、Windows 及び UNIX でのアカウントは従来通り各システムにて管理しており、管理問題については解消されていない。これについては NSS（Name Service Switch）[13]及び LDAP を利用し、ユーザー情報も一元的に管理できることが望ましい。ActiveDirectory の Schema 拡張と NSS との連携について検証を行い、今後のシステム改善につなげたい。

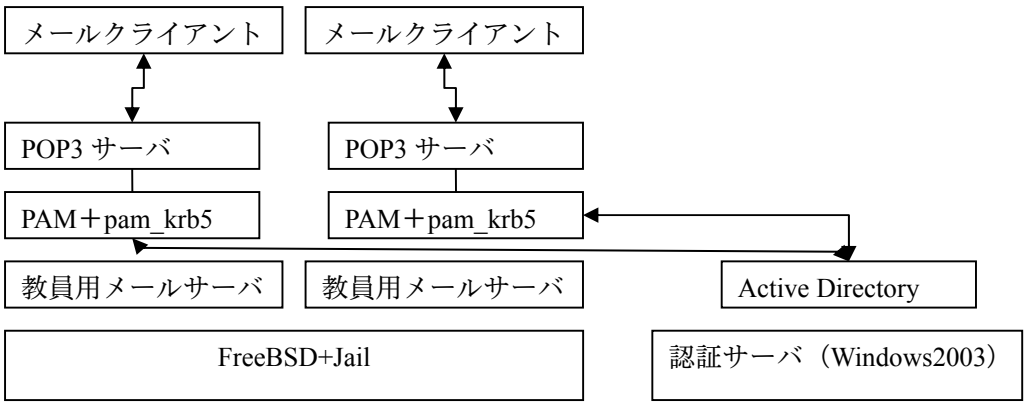

図 1

参考文献（URL）

1 ）高橋基信 「Linux の認証を Active Directory で行う方法」
http://www.monyo.com/technical/windows/kerberos1.html
2 ）Michael Ganss「Single-Sign-On on Linux using LDAP with Active Directory」
http://www.oo-services.com/en/articles/sso.html

雑誌記事

1 ）広瀬雄二 「Jail によるセキュアサーバの環境」UNIX USER 2003.10. P.85-89

注

1 Microsoft が提供する Windows と UNIX の包括的な相互運用を実現するソフト。現在は無償で利用可能。
2 個人またはコンピュータに関する情報を一元的に管理するディレクトリデータベースへアクセスするためのプロトコル
3 Microsoft が提供するディレクトリサーバ
4 Novell が提供するディレクトリサーバ。マルチプラットフォームで利用可能
5 フリーのディレクトリサーバ
6 Apple が提供するディレクトリサーバ。OpenLDAP をベースにしている
7 マサチューセッツ工科大学（MIT）が開発した安全性の高い認証システム。
8 他に LDAP を用いた方法もあるようだが、AD の Schema を拡張しなければならない等の制約やセキュリティを考慮し Kerberos を用いることとした。
9 Post Office Protocol サーバ。一般的にはメールクライアント（MUA）へメールの受け渡しを行う。各個人のメールを扱うためユーザー認証が必要である。
10 Intel が開発したマイクロプロセッサの高速化技術。1 つのプロセッサをあたかも 2 つのプロセッサであるかのように見せかける技術。
11 ハードディスクに記録する際に 2 台以上のディスクを用意し、全部のディスクに同じデータを書き込むことで信頼性を上げる
12 FreeBSD 上に実装されている chroot を強化した仮想環境。chroot ではホスト環境からファイルシステムのみ分離を行うが、jail ではプロセス空間も分離する。
13 従来 UNIX ではユーザー情報は /etc/passwd 等に格納していた。NSS によりユーザ情報に関する問い合わせついて LDAP を用いることができる。